(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－191318

(43)公開日　平成９年(1997)７月22日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	12/46			Ｈ０４Ｌ	11/00	３１０Ｃ
	12/28		7259－5Ｊ	Ｇ０９Ｃ	1/00	６６０Ｅ
Ｇ０９Ｃ	1/00	６６０	7259－5Ｊ			６６０Ｇ
				Ｈ０４Ｌ	9/00	６２１Ｚ
Ｈ０４Ｌ	9/10					６７３Ａ

審査請求　未請求　請求項の数５　ＯＬ　（全 11 頁）　最終頁に続く

(21)出願番号　特願平8－903

(22)出願日　平成８年(1996)１月８日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　松本　達郎
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

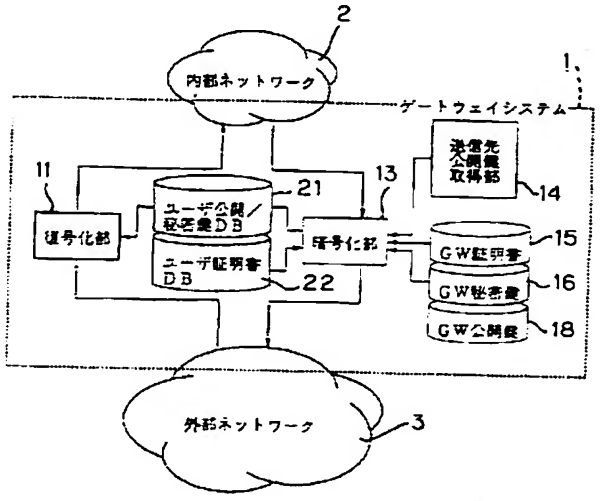
(74)代理人　弁理士　山田　正紀

(54)【発明の名称】　ゲートウェイシステム

(57)【要約】

【課題】本発明は、コンピュータネットワーク上の、あるネットワークと他のネットワークとの間のデータ通信の橋渡しを行なうゲートウェイシステムに関し、通常のプライバシを保つ。

【解決手段】安全性の高いネットワーク２と安全性の低い外部ネットワーク３との間の通信の橋渡しをするゲートウェイシステム１において、内部ネットワーク２から外部ネットワーク３に向けた通信文を、内部ネットワーク２の各ユーザ毎に異なる秘密鍵のうちの発信元のユーザの秘密鍵を用いて暗号化して外部ネットワーク３に送り出し、外部ネットワーク３から内部ネットワーク２に向けた通信文を、内部ネットワーク２の、受信先ユーザの秘密鍵を用いて復号化する。



1

【特許請求の範囲】

【請求項１】　第１の通信回線、および該第１の通信回線を経由してデータ通信を行なう複数の第１の端末を有する第１のネットワークと、第２の通信回線、および該第２の通信回線を経由してデータ通信を行なう複数の第２の端末を有する第２のネットワークとの間のデータ通信の橋渡しを行なうゲートウェイシステムにおいて、

前記第２の通信回線を経由して通信されてきたデータを受信する第１の受信手段と、

前記第１の通信回線にデータを送信する第１の送信手段と、

前記第１の端末それぞれに対応する、相互に異なる秘密鍵が登録された第１のデータベースと、

前記第２の通信回線を経由し前記第１の端末のうちのいずれかの第１の受信端末に向けて送信されてきた、該第１の受信端末の公開鍵で暗号化されたデータを、前記第１のデータベースから読み出した該第１の受信端末の秘密鍵で復号化して前記第１の送信手段に渡す復号化手段とを備えたことを特徴とするゲートウェイシステム。

【請求項２】　前記第１の通信回線を経由して送信されてきたデータを受信する第２の受信手段と、

前記第１の通信回線にデータを送信する第２の送信手段と、

前記第２の端末の公開鍵が登録される第２のデータベースと、

前記第１の通信回線を経由し前記第２の端末のうちのいずれかの第２の受信端末に向けて送信されてきたデータを、前記第２のデータベースから読み出した該第２の受信端末の公開鍵で暗号化して前記第２の送信手段に渡す暗号化手段とを備えたことを特徴とする請求項１記載のゲートウェイシステム。

【請求項３】　前記第２のデータベースに前記第２の受信端末の公開鍵が登録されていない場合に、所定の公開鍵配布局から、該第２の受信端末の公開鍵を取り寄せて登録する送信先公開鍵取得手段を備え、

前記第２のデータベースが、登録された公開鍵を所定期間だけ保持するものであることを特徴とする請求項２記載のゲートウェイシステム。

【請求項４】　前記第１のデータベースは、前記第１の端末の秘密鍵とともに該第１の端末の公開鍵が登録されてなるものであって、

該ゲートウェイシステムが、前記第１の端末の公開鍵を前記第２のネットワークに向けて配布する公開鍵配布手段を備えたことを特徴とする請求項１記載のゲートウェイシステム。

【請求項５】　前記第１のデータベースが、前記復号化手段との間に前記第１の通信回線を介在させた位置に接続されてなることを特徴とする請求項１記載のゲートウェイシステム。

【発明の詳細な説明】

2

【０００１】

【発明の属する技術分野】本発明は、コンピュータネットワーク上の、あるネットワークと他のネットワークとの間のデータ通信の橋渡しを行なうゲートウェイシステムに関する。

【０００２】

【従来の技術】世界的なコンピュータネットワークであるインターネットは、爆発的な勢いでユーザが増え、１９９５年段階では４０００万人に達したと言われている。このようにインターネットが発展してきた背景には、インターネットがオープンなアーキテクチャを採用したことがある。インターネットが注目されるに従って、これをビジネスに使おうというニーズが高まってきている。しかし、インターネットは、オープンなアーキテクチャを採用したことが災いして、ビジネスユースに耐え得るような、通信の秘密が保たれたセキュアな環境になかった。そこで、各種暗号化技術を利用したＰＥＭ（Ｐｒｉｖａｃｙ　Ｅｎｈａｎｃｅｄ　Ｍａｉｌ）やＰＧＰ（Ｐｒｉｔｙ　Ｇｏｏｄ　Ｐｒｉｖａｃｙ）等のプライバシ強化の枠組が提案され、標準化が進みつつあり、これらの枠組を用いれば、インターネットにおいても十分に通信が可能となってきている。

【０００３】一方、パソコン通信のような集中管理型のネットワークは、電話回線等の通信回線を盗聴されない限り、十分にセキュリテイが保たれており、インターネットで使われつつあるプライバシ強化の枠組を使う必要はないと言える。しかし、インターネットとパソコン通信は互いに連携を深め、電子メールその他の通信ツールで、相互乗り入れが可能となってきている。そのため、パソコン通信とインターネットとの間で通信を行なうには、それらの間の橋渡しをするゲートウェイにおいて、セキュリテイに関する何らかの処置が必要になる。具体的には、パソコン通信からインターネットへ出ていく通信には、プライバシ強化の処理を施し、インターネットからパソコン通信へ入ってくる通信には、プライバシ強化がなされている場合は、その処理を解いて、パソコン通信ユーザに見える形にしなければならない。

【０００４】図７は、上記のように構成された従来のゲートウェイシステムの概略構成図である。本図において、内部ネットワーク２は、例えばパソコン通信のような十分にセキュアなネットワーク、外部ネットワーク３は例えばインターネットのような特別なことをしない限り十分にセキュアであるとは言い難いネットワークを指しており、ゲートウェイシステム（以下、「ＧＷ」と略記することがある）１が、それら内部ネットワーク２と外部ネットワーク３との間の橋渡しの役割りを担っている。尚、内部ネットワーク２、外部ネットワーク３は、それぞれ単独のネットワークであってもよいが、それぞれが複数のネットワークの集合体であってもよい。

【０００５】ゲートウェイシステム１は、内部ネットワ

ーク２のある発信端末からの通信文を受け取ると、それを暗号化して外部ネットワーク３に送り出す。電子メールの場合、前述のＰＥＭを用いるとすると、暗号化部１３において、共有鍵暗号系の鍵（共有鍵）によってメール本文を暗号化し、また、送信先証明書取得部１４において何らかの方法で送信先の証明書を手に入れ、その送信先証明書から送信先の公開鍵暗号系の公開鍵を取り出し、その取り出した送信先の公開鍵によって、メール本文の暗号化に用いた共有鍵を暗号化し、さらに、これら暗号化されたメール本文および共有鍵に加え、さらに、公開鍵暗号系の秘密鍵（ＧＷ秘密鍵）１６によって作成した電子署名と、ゲートウェイの証明書（ＧＷ証明書）１５（ないし、そのＧＷ証明書１５に加え、ＧＷ証明書１５を発行した機関の証明書）を統合して外部ネットワーク３へ送出する。

【０００６】外部ネットワーク３側の受信端末では、受け取ったメール中の、自分の公開鍵で暗号化された共有鍵を自分の秘密鍵で復号化し、その復号化された共有鍵でメール本文を復号化する。さらに、ゲートウェイシステム１の公開鍵（ＧＷ公開鍵１８）は、外部ネットワーク３の端末からの要求に応じて配布されるものであり、外部ネットワーク３の受信端末ではその配布されたＧＷ公開鍵によってメールの電子署名を復号化し、そのメールが真正なものであることを確認する。

【０００７】一方、外部ネットワーク３から内部ネットワーク２へ通信を行なう場合、外部ネットワーク３の発信端末では、共有鍵によって通信文を暗号化し、手に入れたＧＷ公開鍵によって、通信文の暗号化に用いた共有鍵を暗号化し、これら暗号化された通信文および共有鍵に、さらに電子署名、発信元の証明書、その証明書発行元の証明書等を付加して、ゲートウェイシステム１に送信する。

【０００８】ゲートウェイシステム１の復号化部１１では、受け取ったメール中の暗号化された共有鍵をＧＷ秘密鍵１６によって復号化し、その復号化された共有鍵でメール本文を復号化する。さらに電子署名のチェックを行ない、署名に間違いがなければ内部ネットワーク２へ通信文を送信する。内部ネットワーク２の受信端末では、ゲートウェイシステム１で既に復号化された通信文を受け取ることができ、そのままその通信文を読むことができる。

【０００９】

【発明が解決しようとする課題】ところで、インターネットの場合、悪意のユーザによって、通信の送信先が改ざんされる恐れがある。図７に示す外部ネットワーク３のユーザＡ（端末Ａ）が内部ネットワークのユーザＢ（端末Ｂ）に向けて通信文を送信した場合、外部ネットワーク上の悪意のユーザＣが、その通信文の宛先を、ユーザＣがコントロールすることのできる、内部ネットワーク２のユーザＤへと書き換えた場合、外部ネットワーク上のユーザＡからの通信文は内部ネットワーク上のユーザＢには届かずにユーザＤに届き、ユーザＣに洩れてしまい、ユーザＡからユーザＢに宛てた通信文のプライバシが守れなくなってしまうという問題がある。

【００１０】本発明は、上記事情に鑑み、通信の秘密が高度に保たれたゲートウェイシステムを提供することを目的とする。

【００１１】

【課題を解決するための手段】上記目的を達成する本発明のゲートウェイシステムは、第１の通信回線、およびその第１の通信回線を経由してデータ通信を行なう複数の第１の端末を有する第１のネットワークと、第２の通信回線、およびその第２の通信回線を経由してデータ通信を行なう複数の第２の端末を有する第２のネットワークとの間のデータ通信の橋渡しを行なうゲートウェイシステムにおいて、上記第２の通信回線を経由して通信されてきたデータを受信する第１の受信手段と、上記第１の通信回線にデータを送信する第１の送信手段と、上記第１の端末それぞれに対応する、相互に異なる秘密鍵が登録された第１のデータベースと、上記第２の通信回線を経由し上記第１の端末のうちのいずれかの第１の受信端末に向けて送信されてきた、その第１の受信端末の公開鍵で暗号化されたデータを、上記第１のデータベースから読み出した第１の受信端末の秘密鍵で復号化して上記第１の送信手段に渡す復号化手段とを備えたことを特徴とする。

【００１２】ここで、上記本発明のゲートウェイシステムは、さらに、上記第１の通信回線を経由して送信されてきたデータを受信する第２の受信手段と、上記第１の通信回線にデータを送信する第２の送信手段と、上記第２の端末の公開鍵が登録される第２のデータベースと、上記第１の通信回線を経由し上記第２の端末のうちのいずれかの第２の受信端末に向けて送信されてきたデータを、上記第２のデータベースから読み出した第２の受信端末の公開鍵で暗号化して上記第２の送信手段に渡す暗号化手段とを備えることが好ましい。

【００１３】また、上記本発明がゲートウェイシステムにおいて、上記第２のデータベースに上記第２の受信端末の公開鍵が登録されていない場合に、所定の公開鍵配布局から、その第２の受信端末の公開鍵を取り寄せて登録する送信先公開鍵取得手段を備え、上記第２のデータベースが、登録された公開鍵を所定期間だけ保持するものであることが好ましい。

【００１４】さらに、上記本発明のゲートウェイシステムにおいて、上記第１のデータベースは、上記第１の端末の秘密鍵とともにその第１の端末の公開鍵が登録されてなるものであって、そのゲートウェイシステムが、上記第１の端末の公開鍵を上記第２のネットワークに向けて配布する公開鍵配布手段を備えることも好ましい態様である。

【００１５】また、上記本発明のゲートウェイシステムが、上記第１の通信回路に接続された第１の端末に変動があった場合に、その第１の端末の変動に応じて上記第１のデータベースの登録内容を更新するデータベース更新手段を備えることも好ましい態様である。さらに、上記本発明のゲートウェイシステムにおいて、上記第１のデータベースが、上記復号化手段との間に上記第１の通信回線を介在させた位置に接続されてなることも好ましい態様である。

【００１６】

【発明の実施の形態】以下、本発明の実施形態について説明する。図１は、本発明のゲートウェイシステムの第１実施形態の概略構成図である。この図１、および後述する各図において、その図よりも先に説明した図に示したゲートウェイシステムの構成要素と同一の構成要素には、先に説明した図に付した番号と同一の符号を付して示し重複説明は省略し、相違点のみ説明する。

【００１７】この図１に示すゲートウェイシステム１には、内部ネットワーク２のユーザ（端末）毎に異なる公開鍵、秘密鍵が登録されたユーザ公開／秘密鍵データベース２１と、内部ネットワーク２のユーザの証明書が登録されたユーザ証明書データベース２２が備えられている。内部ネットワーク２側のある発信端末から外部ネットワーク側のある受信端末に向けて通信文が発信されその通信文をゲートウェイシステム１が受け取ると、ゲートウェイシステム１では、その暗号化部１３において、送信先公開鍵取得部１４によって得られる送信先の公開鍵を用いてその受け取った通信分を暗号化し、外部ネットワークへ送り出すが、その際、ユーザ証明書データベース２２から読み出した発信元のユーザの証明書、ＧＷ証明書１５、および、ユーザ公開／秘密鍵データベース２２から読み出した発信元ユーザの秘密鍵ないしＧＷ秘密鍵を用いた電子署名が付加される。

【００１８】外部ネットワーク側の受信端末では、ゲートウェイシステム１で暗号化された通信文を受け取ると、その通信文を、ゲートウェイの公開鍵および発信元ユーザの公開鍵を用いて復号化する。一方、外部ネットワーク３側から内部ネットワーク２へ通信文を送る際、外部ネットワーク３側の発信端末では、内部ネットワーク２側の受信端末に固有の公開鍵を入手し、その公開鍵を用いて通信文を暗号化して送り出す。ゲートウェイシステム１では、ユーザ公開／秘密鍵データベース２１から送信先ユーザの秘密鍵を読み出してその秘密鍵を用いて通信文を復号化し、内部ネットワーク７２の受信端末に向けて送り出す。

【００１９】このように、図１に示す第１実施形態では、ゲートウェイシステム１上に、内部ネットワーク２のユーザ毎に異なる秘密鍵を保持しているため、セキュアでない外部ネットワーク３の悪意の第三者によって通信の送信先が改ざんされても、内部ネットワーク２の正当な受信先のユーザしか通信文を読むことができず、通信のプライバシが確保される。

【００２０】図２は、本発明のゲートウェイシステムの第２実施形態の概略構成図である。図１に示す第１実施形態との相違点について説明する。図２において、ユーザ登録管理サーバ２０は、内部ネットワーク２中の登録されたユーザの管理を行なう。ユーザ登録時には、ユーザ登録管理部２０２は、ユーザ情報データベース２０１へユーザ情報を登録する。また、ユーザ登録管理部２０２は、ゲートウェイシステム１に対して、ユーザ情報を送り、ユーザ公開／秘密鍵生成部２１０は、送られてきたユーザ情報に基づいて、ユーザ固有の公開／秘密鍵ペアを生成し、ユーザ公開／秘密データベース２１へ登録する。さらにユーザ証明書発行部２３０は、ユーザ情報とユーザの公開鍵からユーザの証明書を発行（生成）し、ユーザ証明書データベース２２へ登録する。

【００２１】この第２実施形態によれば、内部ネットワーク２のユーザの加入、変更に容易に対処できる。図３は、本発明のゲートウェイシステムの第３の実施形態の概略構成図である。図１に示す第１実施形態との相違点について説明する。図３において、公開鍵（証明書）配布部１９は、外部ネットワーク３からの公開鍵（証明書）配布要求を受けて、ユーザ公開鍵／秘密鍵ＤＢデータベース２１から読み出したユーザ公開鍵またはユーザ証明書データベース２２から読み出したユーザ証明書、ＧＷ公開鍵１８またはＧＷ証明書１５の配布を行なう。

【００２２】このように、ゲートウェイシステム１に、内部ネットワーク２および自分自身の公開鍵を配布する公開鍵配布局を兼ねさせてもよい。図４は、本発明のゲートウェイシステムの第４実施形態の概略構成図である。この実施形態では、内部ネットワーク２側のユーザの証明書を管理するユーザ証明書管理サーバ２３、同じく内部ネットワーク２側のユーザ毎の公開鍵、秘密鍵を管理するユーザ公開／秘密鍵管理サーバ２４、ゲートウェイシステム１の秘密鍵を管理するＧＷ秘密鍵管理サーバ２５、およびゲートウェイシステム１の証明書を管理するＧＷ証明書管理サーバ２６は、いずれも内部ネットワーク２の中に配置されている。

【００２３】図４において、内部ネットワーク２から外部ネットワーク３への通信時は、送信先公開鍵取得部１４が何らかの手段で送信先の公開鍵を入手し、その鍵によって通信文（もしくは一時的な共有鍵）を暗号化する。さらに、ＧＷ証明書取得部１００は内部ネットワーク中のＧＷ証明書管理サーバ２６と通信を行ない、ＧＷ証明書管理サーバ２６上のＧＷ証明書管理部２６１を通して、ＧＷ証明書２６０を取得する。また、ＧＷ秘密鍵取得部１６０は内部ネットワーク２中のＧＷ秘密鍵管理サーバ２５と通信を行ない、ＧＷ秘密鍵管理サーバ上のＧＷ秘密鍵管理部２５を通して、ＧＷ秘密鍵２５０を取得する。ユーザ証明書取得部２２０は内部ネットワーク

２中のユーザ証明書管理サーバ２３と通信を行ない。ユーザ証明書管理サーバ２３上のユーザ証明書管理部２３１を通して、ユーザ証明書データベース２３０から読み出されたユーザ証明書を取得する。また、ユーザ秘密鍵取得部２１０は内部ネットワーク２中のユーザ公開／秘密鍵管理サーバ２４と通信を行ない、ユーザ公開／秘密鍵管理サーバ２４上のユーザ秘密鍵管理部２４１を通して、ユーザ公開／秘密鍵データベース２４０から読み出されたユーザ秘密鍵を取得する。最終的に、暗号化通信文、ユーザ秘密鍵またはＧＷ秘密鍵による電子署名、ユーザ証明書、ＧＷ証明書を統合し、外部ネットワーク３へ送信する。

【００２４】外部ネットワーク３から内部ネットワーク２への通信の場合は、受信先のユーザの秘密鍵を得るために、ユーザ秘密鍵取得部２１０は内部ネットワーク２中のユーザ公開／秘密鍵管理サーバ２４と通信を行ない、ユーザ公開／秘密鍵管理サーバ２４上のユーザ秘密鍵管理部２４１を通してユーザ秘密鍵を取得する。復号化部１１では、通信文を秘密鍵によって復号化し、平文を内部ネットワーク２の受信先へ送信する。

【００２５】この図２に示す実施形態では、セキュアでない外部ネットワーク３にさらされるゲートウェイシステム本体部１ａ上ではなく、セキュアな内部ネットワーク２上に暗号鍵を管理するサーバを置き、ゲートウェイシステム本体部１ａはそのサーバと通信を行ない各種の鍵や証明書を取得するので、外部ネットワーク３からの悪意のユーザによる攻撃によっても暗号鍵が漏洩しにくく、内部ネットワーク２をセキュアな環境に保つことができる。

【００２６】図５は、本発明のゲートウェイシステムの一実施形態の、内部ネットワークから外部ネットワークに向けて通信文を送信する部分の詳細ブロック図である。図５において、受信部１３０は内部ネットワークからの通信文を受け取る。送信先解析部１４０は通信文の送信先を解析し、公開鍵読出部１４１は送信先公開鍵データベース１４２から送信先の公開鍵を読み出す。この時、送信先公開鍵データベース１４２に送信先の公開鍵が登録されていない場合、公開鍵要求部１４４に対して、公開鍵を外部ネットワーク３から取得するように指令を出す。公開鍵要求部１４４は外部ネットワーク上の公開鍵配布局３０に対して、送信先の公開鍵を要求し、送信先の公開鍵を取得し、さらに公開鍵登録部１４３に取得した送信先公開鍵データベース１４２への登録を依頼し、公開鍵登録部１４３は登録を依頼された送信先公開鍵を送信先公開鍵データベース１４２に登録する。

【００２７】公開鍵登録部１４３は、送信先公開鍵データベース１４２に送信先公開鍵を登録した時点から起算して一定時間経過すると、その登録した送信先公開鍵を送信先公開鍵データベース１４２から抹消する。こうすることにより、使用されなくなった送信先公開鍵がいつまでも送信先公開鍵データベース１４２のメモリ領域を占有するのが防止される。

【００２８】共有鍵生成部１３２は、一時的に有効な共有鍵をランダムに生成する。共有鍵系暗号化部１３１は共有鍵によって通信文本文を暗号化する。また共有鍵自体は公開鍵暗号化部１３３において、送信先公開鍵によって暗号化される。また、電子署名部１３４は、通信文本文を一方向性のハッシュ関数（ＭＤ５等）にかけ、さらにそれをＧＷ秘密鍵１６で暗号化する。もしくは、図５に点線で示すようにユーザの秘密鍵で暗号化してもよい。最終的に、統合部１３５が、暗号化本文、暗号化共有鍵、電子署名、ＧＷ証明書１５、ユーザ証明書データベース２２から読出した発信元ユーザ証明書を結合し、その結合された通信文を、送信部１３６が外部ネットワークへ送り出す。

【００２９】この図５に示す実施形態によれば、一度取得した送信先公開鍵が送信先公開鍵データベース１４２によって管理されるので、同一の送信先へ通信文を送る場合、外部ネットワークの公開鍵配布局３０への公開鍵取得要求が一度で済み、効率的な暗号通信が可能になる。図６は、本発明のゲートウェイシステムの一実施形態の、外部ネットワークから内部ネットワークに向けて通信文を送信する部分の詳細ブロック図である。

【００３０】図６において、受信部１１０は外部ネットワークから内部ネットワークへの通信文を受け取る。分割部１１１は通信文に含まれている種々の情報を分割する。受信先解析部１１２は内部ネットワーク中の受信先ユーザを解析する。秘密鍵読出部１１３は受信先ユーザの秘密鍵をユーザ公開／秘密鍵ＤＢデータベース２１から読み出す。公開鍵系復号化部１１４は分割部１１１から渡される暗号化共有鍵を受信先ユーザの秘密鍵で復号化し、共有鍵を取り出す。共有鍵系復号化部１１５は取り出された共有鍵を用いて、暗号化本文を復号化し平文に戻す。発信元証明書検査部１１６は証明書発行元の公開鍵を用いて発信元証明書の正当性を検査し、発信元の公開鍵を取り出す。電子署名検査部１１７は電子署名を発信元の公開鍵で復号化し、発信元で通信本文にハッシュ関数にかけた結果を取り出す。さらに、通信文本文の内容が改ざんされていないことを確認するために、電子署名から取り出された結果と、共有鍵系復号化部１１５で得られた通信文本文に対してハッシュ関数をかけた結果とを比較する。それらの結果が同一であれば、送信部１１８は内部ネットワーク中の受信先ユーザに向けて通信文を送信する。

【００３１】この図６に示す実施形態によると、通信文を、内部ネットワークのユーザ毎の秘密鍵によって復号化するので、セキュアでない外部ネットワークの悪意の第三者が送信先を改ざんしても、内部ネットワーク内の正当な受信者に送信される通信文しか正しく復号できないため、通信文のプライバシが守られる。

9　　10

【００３２】

【発明の効果】以上説明したように、本発明によれば、通信文のプライバシが守られた安全性の高いゲートウェイシステムが構築される。

【図面の簡単な説明】

【図１】本発明のゲートウェイシステムの第１実施形態の概略構成図である。

【図２】本発明のゲートウェイシステムの第２実施形態の概略構成図である。

【図３】本発明のゲートウェイシステムの第３実施形態の概略構成図である。

【図４】本発明のゲートウェイシステムの第４実施形態の概略構成図である。

【図５】本発明のゲートウェイシステムの一実施形態の、内部ネットワークから外部ネットワークに向けて通信文を送信する部分の詳細ブロック図である。

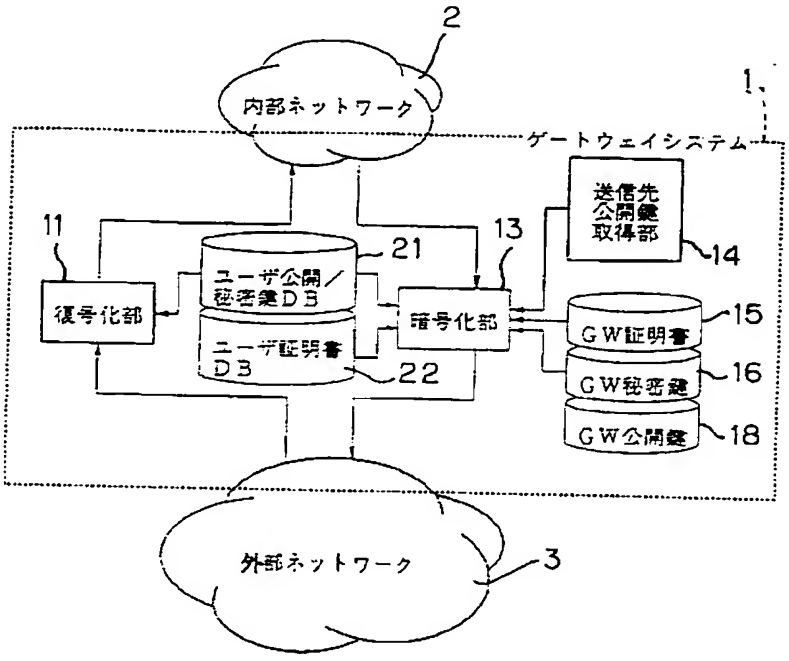
【図６】本発明のゲートウェイシステムの一実施形態の、外部ネットワークから内部ネットワークに向けて通信文を送信する部分の詳細ブロック図である。

【図７】従来のゲートウェイシステムの概略構成図である。

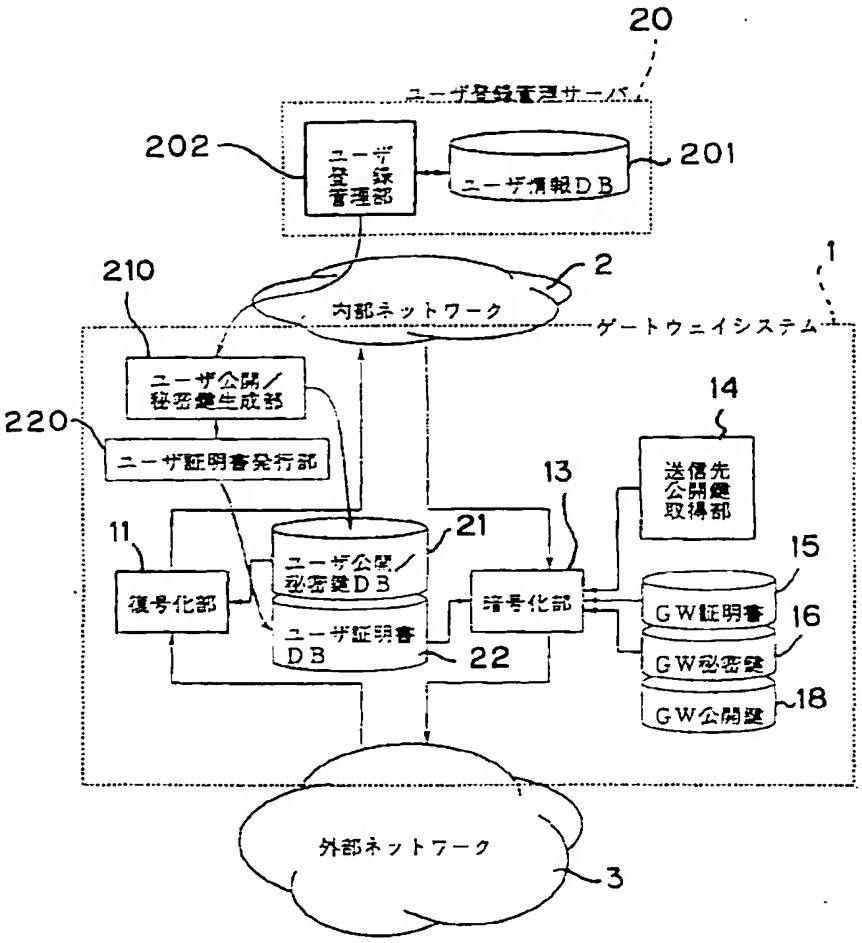
【符号の説明】

１	ゲートウェイシステム
１ａ	ゲートウェイシステム本体部
２	内部ネットワーク
３	外部ネットワーク
１１	復号化部
１３	暗号化部
１４	送信先証明書取得部
１５	ＧＷ証明書
１６	ＧＷ秘密鍵
１８	ＧＷ公開鍵
１９	公開鍵（証明書）配布部
２０	ユーザ登録管理サーバ
２１	ユーザ公開／秘密鍵データベース
２２	ユーザ証明書データベース
２３	ユーザ証明書管理サーバ
２４	ユーザ公開／秘密鍵管理サーバ
２５	ＧＷ秘密鍵管理サーバ
２６	ＧＷ証明書管理サーバ
３０	公開鍵配布局

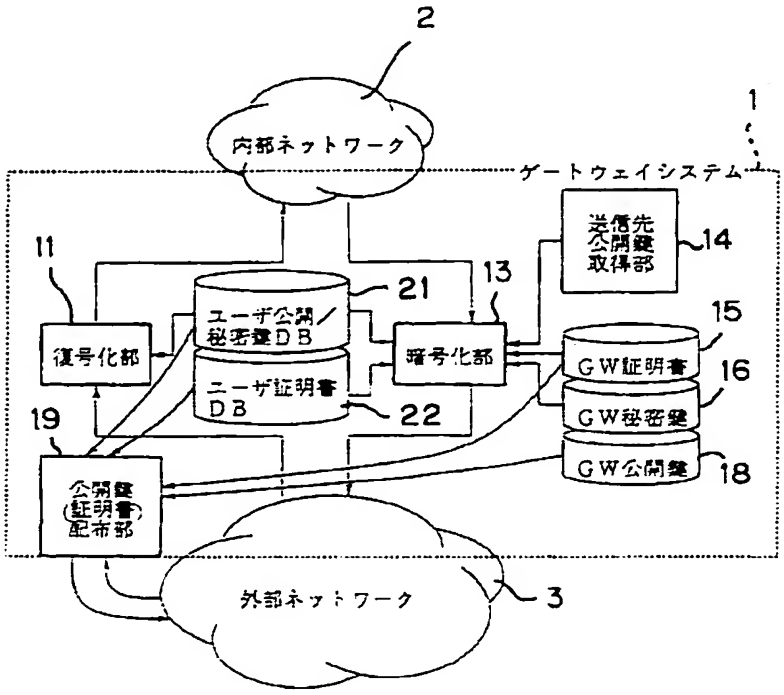
【図１】



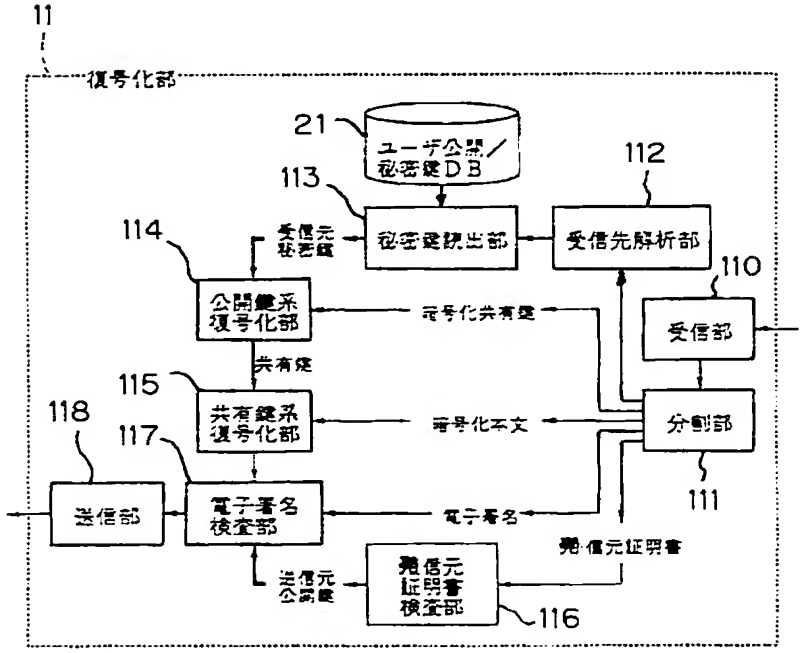
【図2】


20
ユーザ登録管理サーバ
202
ユーザ登録管理部
ユーザ情報DB
201
210
2
内部ネットワーク
1
ゲートウェイシステム
ユーザ公開／秘密鍵生成部
220
ユーザ証明書発行部
14
送信先公開鍵取得部
13
11
21
ユーザ公開／秘密鍵DB
15
復号化部
暗号化部
GW証明書
16
ユーザ証明書DB
22
GW秘密鍵
GW公開鍵
18
外部ネットワーク
3

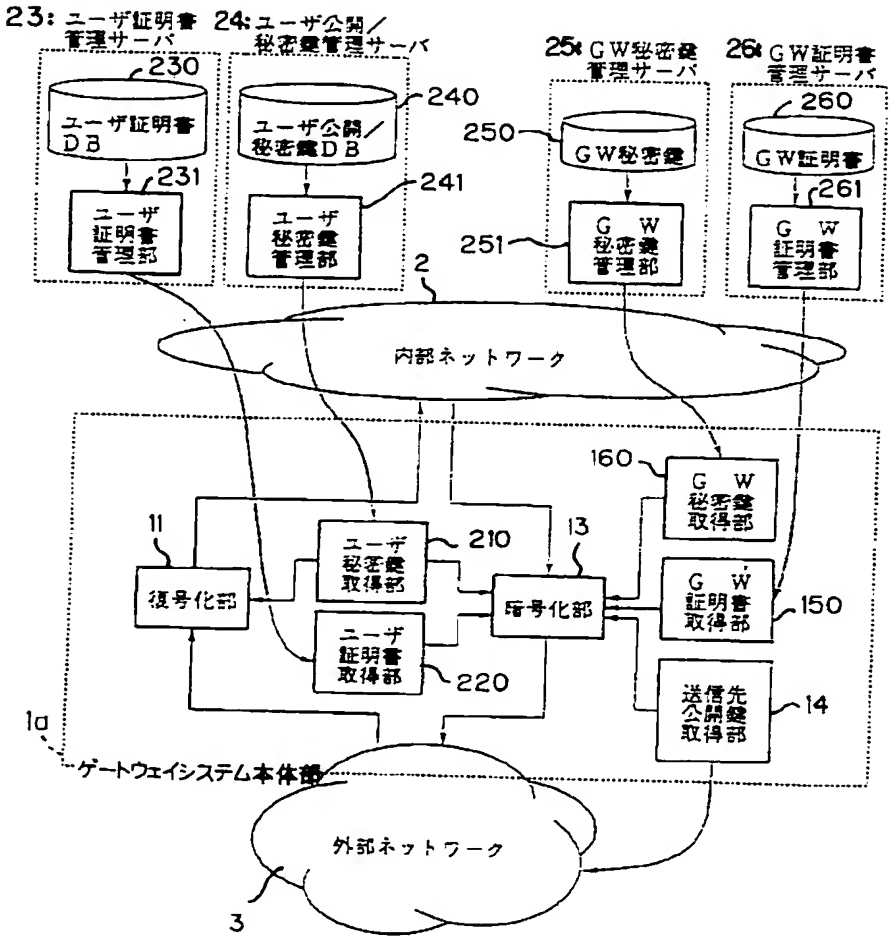
【図3】


2
内部ネットワーク
1
ゲートウェイシステム
11
21
13
送信先公開鍵取得部
14
ユーザ公開／秘密鍵DB
復号化部
暗号化部
15
GW証明書
16
ユーザ証明書DB
22
GW秘密鍵
19
GW公開鍵
18
公開鍵証明書配布部
外部ネットワーク
3

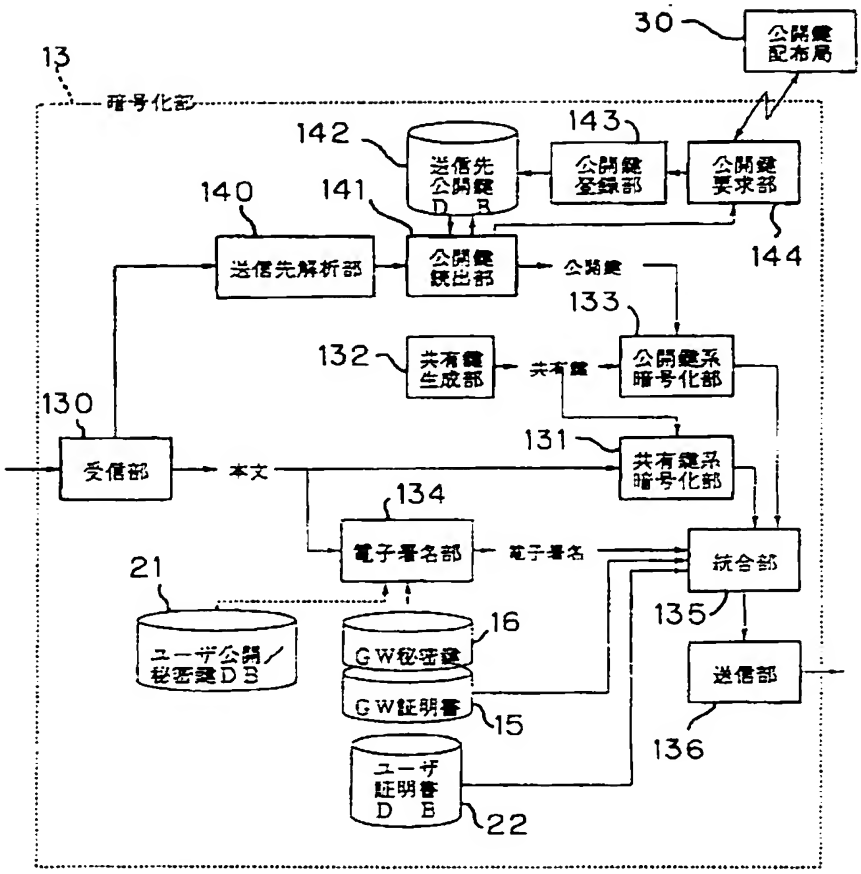
【図6】


11
復号化部
21
ユーザ公開／秘密鍵DB
113
112
秘密鍵読出部
受信先解析部
受信元秘密鍵
114
公開鍵系復号化部
暗号化共有鍵
110
受信部
共有鍵
115
共有鍵系復号化部
暗号化本文
分割部
118
117
送信部
電子署名検査部
電子署名
111
発信元証明書
送信元公開鍵
発信元証明書検査部
116

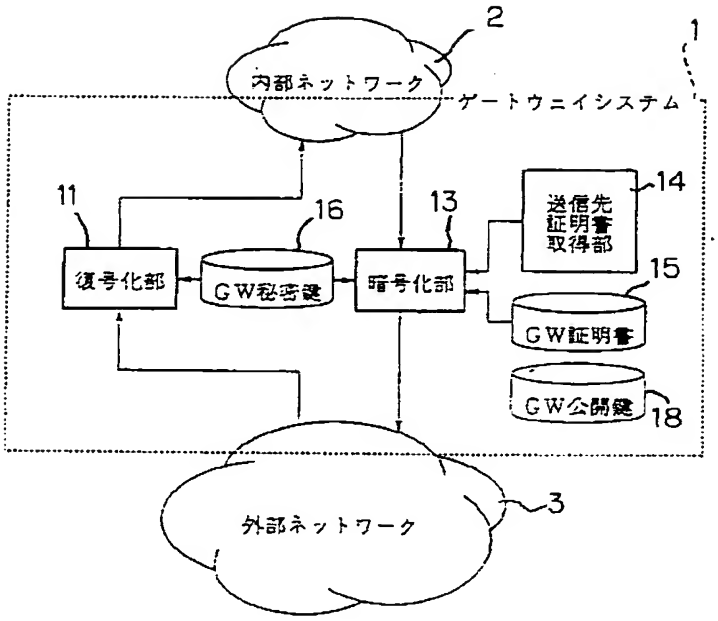
【図４】


23: ユーザ証明書管理サーバ
24: ユーザ公開／秘密鍵管理サーバ
25: GW秘密鍵管理サーバ
26: GW証明書管理サーバ
230
ユーザ証明書DB
231
ユーザ証明書管理部
240
ユーザ公開／秘密鍵DB
241
ユーザ秘密鍵管理部
250
GW秘密鍵
251
GW秘密鍵管理部
260
GW証明書
261
GW証明書管理部
2
内部ネットワーク
160
GW秘密鍵取得部
11
復号化部
ユーザ秘密鍵取得部
210
13
暗号化部
GW証明書取得部
150
ユーザ証明書取得部
220
送信先公開鍵取得部
14
1a
ゲートウェイシステム本体部
外部ネットワーク
3

【図5】


30
公開鍵配布局
13
暗号化部
142
送信先公開鍵DB
143
公開鍵登録部
公開鍵要求部
140
141
144
送信先解析部
公開鍵読出部
公開鍵
133
132
共有鍵生成部
共有鍵
公開鍵系暗号化部
130
131
受信部
本文
共有鍵系暗号化部
134
電子署名部
電子署名
統合部
21
16
135
ユーザ公開/秘密鍵DB
GW秘密鍵
送信部
GW証明書
15
136
ユーザ証明書DB
22

【図７】



フロントページの続き

(51) Int.Cl.[6]		識別記号	庁内整理番号	F I		技術表示箇所
Ｈ０４Ｌ	9/32		9466－5K	Ｈ０４Ｌ	11/20	B
	12/66					

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-191318

(43)Date of publication of application : 22.07.1997

(51)Int.Cl. H04L 12/46

H04L 12/28

G09C 1/00

H04L 9/10

H04L 9/32

H04L 12/66

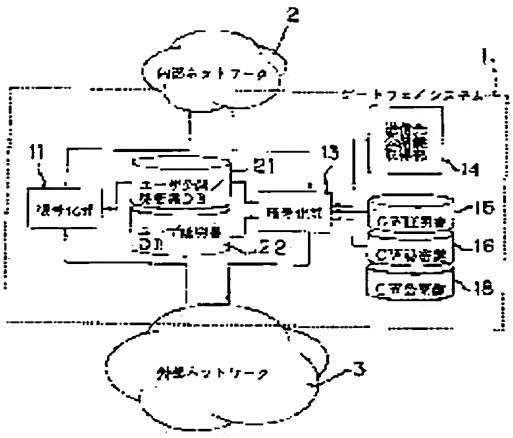
(21)Application number : 08-000903

(22)Date of filing : 08.01.1996

(71)Applicant : FUJITSU LTD

(72)Inventor : MATSUMOTO TATSURO

(54) GATEWAY SYSTEM



(57)Abstract:
PROBLEM TO BE SOLVED: To keep a usual privacy with respect to the gateway system mediating data communication a network on a computer network and other network.
SOLUTION: This system mediates a network 2 with high security and an external network 3 with low security. A communication text from the internal network 2 to the external network 3 is ciphered by using a secret key of a sender user among secret keys different from each user of the internal network 2 and sent to the external network 3, and the control means text from the external network 3 to the internal network 2 is decoded by using a secret key of a reception destination user in the internal network 2.

LEGAL STATUS

[Date of request for examination]	26.02.2001
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3431745
[Date of registration]	23.05.2003
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

CLAIMS

[Claim(s)]
[Claim 1] The 1st network which has two or more 1st terminals which perform data communication via the 1st communication line and this 1st communication line, In the gateway system which mediates between the data communication between the 2nd network which has two or more 2nd terminals which perform data communication via the 2nd communication line and this 2nd communication line The 1st receiving means which receives the data which have communicated via said 2nd communication line, The 1st transmitting means which transmits data to said 1st communication line, and the 1st database with which a private key corresponding to said each of 1st terminal which is mutually different was registered, Have been transmitted towards the 1st accepting station of either of said 1st terminal via said 2nd communication line. The gateway system characterized by having a decryption means to decrypt the data enciphered with the public key of this 1st accepting station with the private key of this 1st accepting station read from said 1st database, and to pass them to said 1st transmitting means.
[Claim 2] The 2nd receiving means which receives the data transmitted via said 1st communication line, The 2nd transmitting means which transmits data to said 1st communication line, and the 2nd database with which the public key of said 2nd terminal is registered, The data transmitted towards the 2nd accepting station of either of said 2nd terminal via said 1st communication line The gateway system according to claim 1 characterized by having the encryption means which enciphers with the public key of this 2nd accepting station read from said 2nd database, and is passed to said 2nd transmitting means.
[Claim 3] The gateway system according to claim 2 by which it has a transmission place public key acquisition means to order and register the public key of this 2nd

accepting station from a predetermined public key distribution station when the public key of said 2nd accepting station is not registered into said 2nd database, and said 2nd database is characterized by being that to which only a predetermined period holds the registered public key.

[Claim 4] Said 1st database is a gateway system according to claim 1 characterized by having a public key distribution means by which come to register the public key of this 1st terminal, and this gateway system turns the public key of said 1st terminal to said 2nd network, and distributes it with the private key of said 1st terminal.

[Claim 5] The gateway system according to claim 1 characterized by coming to connect said 1st database with the location which made said 1st communication line intervene between said decryption means.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the gateway system which mediates between the data communication between a certain network on a computer network, and other networks.

[0002]

[Description of the Prior Art] The user of Internet which is a global computer network increases with explosive vigor, and it is said that it amounted to 40 million people in the phase in 1995. Thus, the Internet has adopted open architecture as the background into which the Internet has developed. The needs that this will be used for business have been increasing as the Internet attracts attention. However, having adopted open architecture suffered misfortune and there was no Internet in the secure environment where the communicative secret that a business youth could be borne was maintained. Then, if the framework of privacy strengthening, such as PEM (Privacy Enhanced Mail) using various encoding technology and PGP (Prity Good Privacy), is proposed, a standardization is progressing and these frameworks are used, also in the Internet, a communication link will become fully possible.

[0003] On the other hand, security is fully maintained and the network of a centralized-control mold like personal computer communications can be said to be not using the framework of privacy strengthening currently used by the Internet, unless communication lines, such as the telephone line, are intercepted. However, the

Internet and personal computer communications promote cooperation mutually, are the communication link tool of an electronic mail and others, and are becoming exchangeable. Therefore, in order to communicate between personal computer communications and the Internet, in the gateway which carries out mediation between them, a certain treatment about security is needed. Privacy strengthening is processed for the communication link left from personal computer communications to the Internet, and when privacy strengthening is made by the communication link which comes into personal computer communications from the Internet, the processing must be solved and, specifically, it must be made the form which is in sight of a personal-computer-communications user.

[0004] Drawing 7 is the outline block diagram of the conventional gateway system constituted as mentioned above. In this Fig., the network which is hard to say that the internal network 2 is fully secure unless a special thing [like the Internet] whose network secure enough like personal computer communications and external network 3 are is done is pointed out, and the gateway system (it may be hereafter written as "GW") 1 is bearing the role rate of mediation between these interior network 2 and the external network 3. In addition, although the internal network 2 and the external network 3 may be respectively independent networks, each may be the aggregate of two or more networks.

[0005] If the correspondence from a master station with the internal network 2 is received, the gateway system 1 will encipher it and will send it out to the external network 3. Supposing it uses the above-mentioned PEM in the case of an electronic mail, it will set in the encryption section 13. The e-mail text is enciphered with the key (share key) of a shared key encryptosystem system. Again In the transmission place certificate acquisition section 14, the certificate of a transmission place is got by a certain approach, and the public key of the public-key-encryption system of a transmission place is picked out from the transmission place certificate. With the taken-out public key of a transmission place The electronic signature which was further created with the private key (GW private key) 16 of a public-key-encryption system in addition to the e-mail text and the share key which enciphered the share key used for encryption of the e-mail text, and were these-enciphered further, The certificate (GW certificate) 15 (or certificate of the engine which published the GW certificate 15 in addition to the GW certificate 15) of the gateway is unified, and it sends out to the external network 3.

[0006] In the accepting station by the side of the external network 3, the share key enciphered with its own public key under received mail is decrypted with its own

private key, and the e-mail text is decrypted with the decrypted share key. Furthermore, the public key (GW public key 18) of the gateway system 1 is distributed according to the demand from the terminal of the external network 3, decrypts the electronic signature of e-mail with the distributed GW public key in the accepting station of the external network 3, and checks Shinsei [the mail].

[0007] On the other hand, when communicating from the external network 3 to the internal network 2, in the master station of the external network 3, with a share key, correspondence is enciphered, and the share key used for encryption of correspondence is enciphered with got GW public key, and the certificate of electronic signature and dispatch origin, the certificate of the certificate issue origin, etc. are further added to the correspondence and the share key which were these-enciphered, and it transmits to the gateway system 1.

[0008] In the decryption section 11 of the gateway system 1, the share key with which it was enciphered under received mail is decrypted with the GW private key 16, and the e-mail text is decrypted with the decrypted share key. Furthermore electronic signature is checked, and if correct to a signature, correspondence will be transmitted to the internal network 2. In the accepting station of the internal network 2, the correspondence already decrypted by the gateway system 1 can be received, and the correspondence can be read as it is.

[0009]

[Problem(s) to be Solved by the Invention] By the way, in the case of the Internet, there is a possibility that a communicative transmission place may be altered by the malicious user. When the user A of the external network 3 shown in drawing 7 (terminal A) transmits correspondence towards the user B of an internal network (terminal B), User C can control [the user C of the malice on an external network] the destination of the correspondence. When it rewrites to the user D of the internal network 2, the correspondence from the user A on an external network reaches User D, without reaching the user B on an internal network. It leaks to User C and there is a problem of it becoming impossible to protect the privacy of the correspondence addressed to User B from User A.

[0010] This invention aims at offering the gateway system by which the communicative secret was maintained at altitude in view of the above-mentioned situation.

[0011]

[Means for Solving the Problem] The gateway system of this invention which attains the above-mentioned purpose The 1st communication line and the 1st network which

has two or more 1st terminals which perform data communication via the 1st communication line, In the 2nd communication line and the gateway system which mediates between the data communication between the 2nd network which has two or more 2nd terminals which perform data communication via the 2nd communication line The 1st receiving means which receives the data which have communicated via the 2nd communication line of the above, The 1st transmitting means which transmits data to the 1st communication line of the above, and the 1st database with which a private key corresponding to each 1st terminal of the above which is mutually different was registered, Have been transmitted towards the 1st accepting station of either of the 1st terminal of the above via the 2nd communication line of the above. It is characterized by having a decryption means to decrypt the data enciphered with the public key of the 1st accepting station with the private key of the 1st accepting station read from the 1st database of the above, and to pass them to the transmitting means of the above 1st.

[0012] Here the gateway system of above-mentioned this invention Furthermore, the 2nd receiving means which receives the data transmitted via the 1st communication line of the above, The 2nd transmitting means which transmits data to the 1st communication line of the above, and the 2nd database with which the public key of the 2nd terminal of the above is registered, It is desirable to have an encryption means to encipher with the public key of the 2nd accepting station read from the 2nd database of the above, and to pass the data transmitted towards the 2nd accepting station of either of the 2nd terminal of the above via the 1st communication line of the above to the transmitting means of the above 2nd.

[0013] Moreover, above-mentioned this invention is equipped with a transmission place public key acquisition means to order and register the public key of the 2nd accepting station from a predetermined public key distribution station when the public key of the 2nd accepting station of the above is not registered into the 2nd database of the above in the gateway system, and it is desirable that the 2nd database of the above is that to which only a predetermined period holds the registered public key.

[0014] Furthermore, in the gateway system of above-mentioned this invention, the 1st database of the above is a mode also with desirable also having a public key distribution means by which come to register the public key of the 1st terminal, and the gateway system turns the public key of the 1st terminal of the above to the 2nd network of the above, and distributes it with the private key of the 1st terminal of the above.

[0015] Moreover, when the 1st terminal by which the gateway system of

above-mentioned this invention was connected to the 1st communication circuit of the above has fluctuation, it is also a desirable mode to have a data-base-updating means to update the contents of registration of the 1st database of the above according to fluctuation of the 1st terminal. Furthermore, in the gateway system of above-mentioned this invention, it is also a desirable mode to come to connect the 1st database of the above with the location which made the 1st communication line of the above intervene between the above-mentioned decryption means.

[0016]

[Embodiment of the Invention] Hereafter, the operation gestalt of this invention is explained. Drawing 1 is the outline block diagram of the 1st operation gestalt of the gateway system of this invention. In this drawing 1 and each drawing mentioned later, the same sign as the number given to drawing explained previously is attached and shown in the same component as the gateway structure-of-a-system element shown in drawing explained ahead of that drawing, duplication explanation is omitted and only difference explains it.

[0017] The gateway system 1 shown in this drawing 1 is equipped with the user public presentation / private key database 21 with which a public key which is different to every [of the internal network 2] user (terminal), and the private key were registered, and the user certificate database 22 with which the certificate of the user of the internal network 2 was registered. If correspondence is sent towards a certain accepting station by the side of an external network from a certain master station by the side of the internal network 2 and the gateway system 1 receives the correspondence, in the gateway system 1, it will set in the encryption section 13. Although the received communicated part is enciphered using the public key of the transmission place obtained by the transmission place public key acquisition section 14 and being sent out to an external network The electronic signature using a sending agency user's private key thru/or GW private key read from the certificate of the user of the dispatch origin read from the user certificate database 22, the GW certificate 15, and the user public presentation / private key database 22 is added in that case.

[0018] In the accepting station by the side of an external network, if the correspondence enciphered by the gateway system 1 is received, the correspondence will be decrypted using the public key of the gateway, and a sending agency user's public key. On the other hand, in case correspondence is sent to the internal network 2 from the external network 3 side, in the master station by the side of the external network 3, the public key of a proper comes to hand to the accepting station by the side of the internal network 2, and correspondence is enciphered and sent out using

the public key. In the gateway system 1, a transmission place user's private key is read from user public presentation / private key database 21, correspondence is decrypted using the private key, and it sends out towards the accepting station of the internal network 72.

[0019] Thus, with the 1st operation gestalt shown in drawing 1 , on the gateway system 1, since a different private key for every user of the internal network 2 is held, even if a communicative transmission place is altered by the holder in bad faith of the external network 3 which is not secure, only the user of the just reception place of the internal network 2 can read correspondence, but communicative privacy is secured.

[0020] Drawing 2 is the outline block diagram of the 2nd operation gestalt of the gateway system of this invention. Difference with the 1st operation gestalt shown in drawing 1 is explained. In drawing 2 , the user registration management server 20 manages the user by whom it was registered in the internal network 2. At the time of user registration, the user registration Management Department 202 registers User Information to the User Information database 201. Moreover, to the gateway system 1, based on User Information to which User Information has been sent, delivery, and the user public presentation / private key generation section 210 generate public presentation / private key pair of a user proper, and the user registration Management Department 202 registers it to user public presentation / secret database 21. Furthermore, the user certificate issue section 230 publishes a user's certificate from the public key of User Information and a user (generation), and registers it to the user certificate database 22.

[0021] According to this 2nd operation gestalt, subscription of the user of the internal network 2 and modification can be coped with easily. Drawing 3 is the outline block diagram of the 3rd operation gestalt of the gateway system of this invention. Difference with the 1st operation gestalt shown in drawing 1 is explained. In drawing 3 , the public key (certificate) distribution section 19 performs distribution of the user certificate read from the user public key or the user certificate database 22 read from the user public key / private key DB database 21, the GW public key 18, or the GW certificate 15 in response to the public key (certificate) distribution request from the external network 3.

[0022] Thus, the gateway system 1 may be made to serve as the public key distribution station which distributes its own [the internal network 2 and] public key. Drawing 4 is the outline block diagram of the 4th operation gestalt of the gateway system of this invention. With this operation gestalt, the user certificate management server 23 which manages the certificate of the user by the side of the internal

network 2, the user public presentation / private key management server 24 which similarly manages the public key for every user by the side of the internal network 2 and a private key, GW private key management server 25 which manages the private key of the gateway system 1, and GW certificate management server 26 which manages the certificate of the gateway system 1 are arranged by each in the internal network 2.

[0023] In drawing 4 , at the time of the communication link to the external network 3 from the internal network 2, the transmission place public key acquisition section 14 receives the public key of a transmission place with a certain means, and correspondence (or a temporary share key) is enciphered with the key. Furthermore, GW certificate acquisition section 100 communicates with GW certificate management server 26 in an internal network, lets GW certificate Management Department 261 on GW certificate management server 26 pass, and acquires the GW certificate 260. Moreover, GW private key acquisition section 160 communicates with GW private key management server 25 in the internal network 2, lets GW private key Management Department 25 on GW private key management server pass, and acquires the GW private key 250. The user certificate acquisition section 220 is a deed about the user certificate management server 23 in the internal network 2, and a communication link. It lets the user certificate Management Department 231 on the user certificate management server 23 pass, and the user certificate read from the user certificate database 230 is acquired. Moreover, the user private key acquisition section 210 communicates with the user public presentation / private key management server 24 in the internal network 2, lets the user private key Management Department 241 on user public presentation / private key management server 24 pass, and acquires the user private key read from user public presentation / private key database 240. Finally, the electronic signature by encryption correspondence, the user private key, or GW private key, a user certificate, and GW certificate are unified, and it transmits to the external network 3.

[0024] In order [from the external network 3 to the internal network 2] to obtain the private key of the user of a reception place in a communication link, the user private key acquisition section 210 communicates with the user public presentation / private key management server 24 in the internal network 2, and acquires a user private key through the user private key Management Department 241 on user public presentation / private key management server 24. In the decryption section 11, correspondence is decrypted with a private key and a plaintext is transmitted to the reception place of the internal network 2.

[0025] It is not on body section of gateway system 1a exposed to the external network 3 which is not secure with the operation gestalt shown in this drawing 2 . Since the server which manages a cryptographic key is placed on the secure internal network 2, body section of gateway system 1a communicates with the server and various kinds of keys and certificates are acquired Also by the attack by the user of the malice from the external network 3, it is hard to reveal a cryptographic key and the internal network 2 can be maintained at a secure environment.
[0026] Drawing 5 is the detail block diagram of the part which transmits correspondence towards an external network from the internal network of 1 operation gestalt of the gateway system of this invention. In drawing 5 , a receive section 130 receives the correspondence from an internal network. The transmission place analysis section 140 analyzes the transmission place of correspondence, and the public key read-out section 141 reads the public key of a transmission place from the transmission place public key database 142. When the public key of a transmission place is not registered into the transmission place public key database 142 at this time, a command is issued to the public key demand section 144 so that a public key may be acquired from the external network 3. Requesting the registration to the transmission place public key database 142 which the public key demand section 144 required the public key of a transmission place, acquired the public key of a transmission place to the public key distribution station 30 on an external network, and was further acquired in the public key registration section 143, the public key registration section 143 registers into the transmission place public key database 142 the transmission place public key from which registration was requested.
[0027] The public key registration section 143 will delete the registered transmission place public key from the transmission place public key database 142, if fixed time amount progress is measured and carried out from the time of registering a transmission place public key into the transmission place public key database 142. By carrying out like this, it is prevented that the transmission place public key used no longer occupies the memory area of the transmission place public key database 142 forever.
[0028] The share key generation section 132 generates an effective share key at random temporarily. The share key system encryption section 131 enciphers the correspondence text with a share key. Moreover, the share key itself is enciphered with a transmission place public key in the public-key-encryption-ized section 133. Moreover, on the other hand, the electronic signature section 134 applies the correspondence text to the Hash Functions (MD5 etc.) of tropism, and enciphers it

with the GW private key 16 further. Or as a dotted line shows to drawing 5 , you may encipher with a user's private key. Finally the integrated section 135 combines the encryption text, an encryption share key, electronic signature, the GW certificate 15, and the sending agency user certificate read from the user certificate database 22, and the transmitting section 136 sends out the combined correspondence to an external network.

[0029] Since the transmission place public key acquired once is managed by the transmission place public key database 142 according to the operation gestalt shown in this drawing 5 , when sending correspondence to the same transmission place, a public key acquisition demand to the public key distribution office 30 of an external network can be managed with once, and efficient cryptocommunication becomes possible. Drawing 6 is the detail block diagram of the part which transmits correspondence towards an internal network from the external network of 1 operation gestalt of the gateway system of this invention.

[0030] In drawing 6 , a receive section 110 receives the correspondence to an internal network from an external network. The division section 111 divides the various information included in correspondence. The reception place analysis section 112 analyzes the reception place user in an internal network. The private key read-out section 113 reads a reception place user's private key from user public presentation / private key DB database 21. The public key system decryption section 114 decrypts the encryption share key passed from the division section 111 with a reception place user's private key, and takes out a share key. Using the taken-out share key, the share key system decryption section 115 decrypts the encryption text, and returns it to a plaintext. The sending agency certificate Banking Inspection Department 116 inspects the justification of a sending agency certificate using the public key of certificate issue origin, and takes out the public key of a sending agency. The electronic signature Banking Inspection Department 117 decrypts electronic signature with the public key of a sending agency, and takes out the result which is a sending agency and was applied to the communication link text at the Hash Function. Furthermore, in order to check that the contents of the correspondence text are not altered, the result taken out from electronic signature is compared with the result multiplied by the Hash Function to the correspondence text acquired in the share key system decryption section 115. If those results are the same, the transmitting section 118 will transmit correspondence towards the reception place user in an internal network.

[0031] Since correspondence is decrypted with the private key for every user of an

internal network according to the operation gestalt shown in this drawing 6 and only the correspondence transmitted to the just addressee in an internal network can be correctly decoded even if the holder in bad faith of the external network which is not secure alters a transmission place, the privacy of correspondence is protected.

[0032]

[Effect of the Invention] As explained above, according to this invention, the gateway system with high safety by which the privacy of correspondence was protected is built.

[Translation done.]